METHOD AND SYSTEM FOR IDENTIFYING LOST OR STOLEN DEVICES

Background of the Invention

Field of the Invention

The invention relates to a method and system for retrieving lost or stolen devices. More particularly, the invention relates to a method and system for identifying lost or stolen portable computers as they pass through an airport checkpoint.

Discussion of the Related Technology

The theft of portable devices, especially portable electronic devices, continues to be a widespread problem in the United States and world-wide. Each year, millions of dollars worth of electronic equipment such as portable, or laptop, computers are stolen or lost. Typically, when a device is lost or stolen, the owner has no way of retrieving or otherwise locating the device. He or she is then forced to replace the lost item, or make do without it.

Currently existing technology allows devices to be identified by means of radio frequency identification (RFID) tags. RFID technology uses electromagnetic energy (such as radio) as a medium through which information is sent. Referring to Figure 1, an RFID system 100 is illustrated. The RFID system 100 includes an RFID tag 102 for transmitting and/or receiving radio frequency signals and a reader 104 for receiving radio frequency signals from the RFID tag 102 and transmitting radio frequency signals to the RFID tag 102. The system 100 also includes a computer 106 which is coupled to the reader 104 by a communications link 108. The communications link 108 may be any one of various types of well-known communication links such as a cable line that directly connects the reader 104 to the computer 106, an Ethernet communications link, or a modem communications link, for example. Through the communications link 108, the reader 104 can receive commands and data from the computer 106 and, thereafter, send data to the remote RFID tag 102. As was noted above, the reader 104 can also receive data from the remote RFID tag 102 and pass the data back to the computer 102.

RFID technology overcomes many limitations of other automatic identification approaches, such as those using bar codes and infrared technology, which use light to communicate. Since an RFID tag 102 does not require a visual scanner, or other vision system, to detect its presence, it may be hidden or invisible to the eye and may also be used in harsh or dirty environments. A reader 104 reads information transmitted by the RFID tag 102 even if the tag 102 is completely hidden from view.

An RFID tag 102 typically includes a receiver and some type of transmitter, an antenna, and memory. There are two categories of RFID tags - active and passive - that represent two different types of RF communication. Tags without batteries are known as passive tags because they derive their power from the RF energy transmitted from a reader. Passive RFID tags tend to be smaller and exhibit short range transmission characteristics (under six feet), whereas battery-powered, active tags, tend to be larger and exhibit long range transmission characteristics (over one hundred feet).

Active tags send data back to the reader with radio power generated from a battery within the tag. Passive tags, on the other hand, use modulated backscatter (MBS) to transmit reflected energy, dictated by the data stream from the tag, back to the reader. Passive tags using MBS are better suited for gate or lane applications where it is undesirable to wake up (see) any tags beyond a certain distance and where there are few obstructions in the energy path.

With the aid of RFID technology, devices which are brought within range of a reader, or interrogator, may be detected. Furthermore, known devices, such as those on assembly lines, can be identified and their progress tracked using this technology. However, there is currently no method or system which provides a mechanism by which it can be determined if the device being detected is lost or stolen. To accomplish this purpose and to be of value, such a system would not only have to identify the device, but be able to determine that it was, in fact, lost or stolen and thereafter, notify appropriate personnel of the matter. Additionally, the reader of such an anti-theft/retrieval system, would best be strategically located so as to make it likely that a significant number of lost or stolen devices would come within range of the reader.

Therefore, what is needed is a method and system of identifying devices, which are randomly brought within range of a reader, determining if the detected devices are

lost or stolen and thereafter, notifying appropriate security personnel when such device is located.

Summary of the Invention

The invention addresses the above and other needs by providing a method and system which utilizes RFID technology to identify lost or stolen goods that randomly come within range of an RFID reader, and thereafter, notifies security personnel of the lost or stolen status of the goods.

In one embodiment of the invention, a system for identifying a lost or stolen device, includes: a transmitter, coupled to the device, for transmitting identification information; a receiver which receives the identification information transmitted by the transmitter, when the transmitter is within a defined distance from the receiver; and a computer, coupled to the receiver so as to receive the information from the receiver, said computer having a first database for storing data associated with lost or stolen devices, wherein said computer compares the information with the stored data, and generates an alarm if the information matches at least some of the stored data.

In another embodiment, a system for identifying a lost or stolen item, includes: a radio frequency identification device, connected to the item, for transmitting information related to the item; a reader which receives the information transmitted by the radio frequency identification device, when the radio frequency identification device is within a defined distance from the reader; and a computer, coupled to the reader so as to receive the information from the reader, said computer having a database for storing a list of lost or stolen items, wherein the computer compares the information with the list of lost or stolen devices, and generates an alarm if the comparison produces a match.

In another embodiment, a system for identifying lost or stolen goods, includes: means for receiving data transmitted by a radio frequency identification device coupled to an item when the item comes within a defined distance of the means for receiving; means for storing a list of lost or stolen goods; means for comparing the data to the list of lost or stolen goods and determining if the data matches information contained in the list of lost or stolen goods; and means for generating an alarm, if the data matches information contained in the list.

In a further embodiment of the invention, a system for identifying a lost or item includes: means for storing identification information in a memory of a radio frequency identification (RFID) device contained within the item, wherein the RFID device transmits the identification information; means for reporting when the item is lost or stolen; means for receiving the identification information transmitted by the RFID device when the item comes within a defined range of the means for receiving; means for storing data associated with lost or stolen items; means for comparing the received identification information to the data associated with the lost or stolen items and for determining if the identification information indicates that the item is lost or stolen; means for generating an alarm, if the identification information indicates the item is lost or stolen, so as to alert personnel of the lost or stolen status of the item; and means for updating the data associated with the lost or stolen items.

In yet another embodiment, the invention is a method of identifying lost or stolen goods, which includes the acts of: receiving information transmitted by a radio frequency identification (RFID) device, coupled to an item, when the item comes within a defined range of a receiver which receives the information; storing data associated with lost or stolen goods in a database coupled to the receiver; comparing the information to the data and determining if the information matches the data associated with the lost or stolen goods; and generating an alarm, if the information matches the data.

In another embodiment, the method of the invention includes: storing identification information in a memory of a radio frequency identification (RFID) device contained within an item, wherein the RFID device transmits the identification information; maintaining a list of lost or stolen items in a database of a computer; receiving the identification information transmitted by the RFID device when the computer comes within a defined range of a receiver, coupled to the computer; comparing the received identification information to the list of lost or stolen items and determining if the identification information indicates that the item is included in the list of lost or stolen items; and generating an alarm, if the identification information indicates the item is lost or stolen.

Brief Description of the Drawings

Figure 1 is a block diagram illustrating a prior art radio frequency identification (RFID) system in which an RFID tag may be identified with a reader device coupled to a computer.

Figure 2 is a perspective view of an anti-theft/ retrieval system in accordance with one embodiment of the invention.

Figure 3 is a block diagram of a computer network, having multiple readers, for identifying lost or stolen goods, in accordance with one embodiment of the invention.

Figure 4 is a perspective view of a laptop computer having an RFID device embedded within its housing so as to transmit information related to the laptop computer to a receiving device, in accordance with one embodiment of the invention.

Detailed Description of the Invention

The invention is described in detail below with reference to the figures, wherein like elements are referenced with like numerals throughout.

Referring to Figure 2, an anti-theft/retrieval system 200 is illustrated. The system 200 includes a reader 202 coupled to a corridor 204 through which a person 206 may walk. As shown in Figure 2, the person 206 is carrying a device 208 having a transmitter 210 embedded therein. The transmitter 210 transmits information related to the device 208 to the reader 202 when the transmitter 210 is within a defined distance from the reader 202. In this way the reader 202 detects the presence of the device 208 and is able to identify it.

In one embodiment, the corridor 204 may be a metal detector such as those typically located in or near an airport terminal. Alternatively, the corridor 204 may be replaced by an x-ray machine, such as those which are typically located next to a metal detector in an airport, which includes a conveyor belt for transporting items placed thereon under an x-ray scanner.

By placing the RFID reader 202 near the metal detector and/or the x-ray machine of an airport checkpoint, the invention provides a security measure against

persons trying to board a plane with lost or stolen property. Alternatively, or as an additional security measure, a reader 202 may be positioned near a baggage check-in point such that all baggage being loaded into a plane may be screened for lost or stolen devices. Therefore, by placing readers 202 at strategic checkpoints, within an airport, for example, a radio frequency security net/retrieval system is established which can identify lost/stolen items and assist security personnel stationed near each checkpoint in retrieving the lost/stolen devices. As used herein, the term "checkpoint" refers to any location or point in which people and/or items must pass in order to move on to another location or point.

In the scenario described above, it may be preferable to utilize a transmitter 210, and/or reader 202 with a short transmission/reception range, e.g., six feet, so as to not read transmitters that are far away from the reader 202. Since it is an object of the invention to identify a particular item which has been reported to be lost or stolen, it is counter-productive to receive information from multiple transmitters located in different areas. In such a scenario, one could not be sure which transmitter was transmitting information indicating the presence of a lost or stolen item. In one embodiment, the transmitter 210 is a passive RFID tag.

Coupled to the reader 202 is a computer 212 which receives information from the reader 202 and compares the information to a list of lost and/or stolen devices, stored in a database 214 coupled to the computer 212. Upon comparing the information received from the transmitter 210 to the list of lost and/or stolen devices, the computer 212 determines if there is a match. If there is a match, the computer 212 generates an appropriate alarm signal to notify personnel stationed near the location of the reader 202 and corridor 204 of the status of the device 208 so that appropriate action can be taken. As used herein, the term "list" refers to any format in which data, or information may be stored so as to be retrievable for purposes of review and/or analysis.

In one embodiment, the transmitter 210 may be a standard radio frequency identification (RFID) tag which is well-known in the industry. In another embodiment, the transmitter 210 is a MicroStamp ® remote intelligent communications (RIC) device,

manufactured by Micron Communications, Inc. Microstamp ® is a registered trademark for a family of RIC devices that use active and passive transmitters. However, RIC devices differ from traditional RFID devices in that RIC devices typically have a battery, a microprocessor, a high-frequency radio, more memory and longer range capability when compared to standard RFID devices.

The MicroStamp ® RIC device contains a MicroStamp Engine ™ integrated circuit (IC), which combines a direct sequence spread spectrum (DSSS) microwave frequency radio, a microcontroller, and a low power static random access memory (SRAM) into a single chip. The MicroStamp Engine IC, when coupled with an antenna and a battery, forms the MicroStamp RIC device. Because the IC combines hundreds of thousands of components on one small chip, the MicroStamp RIC device may be assembled, with a small battery, into very small packages, making it ideal for applications in small handheld, or portable, electronic devices. Although RIC devices are typically more advanced than standard RFID tags, as used herein, the term "radio frequency identification," or "RFID tag", or "RFID device", and any combination or conjugation thereof, refers to both standard RFID devices and RIC devices as described above, as well as any radio frequency transmission device, capable of transmitting data for identification purposes to a receiver.

In one embodiment, the reader 202 is a MicroStamp®4000 RF Interrogator, manufactured by Micron Communications, Inc. The function of this interrogator 202 is twofold: 1) it receives commands and data from the computer 212 and sends data packets to the remote intelligent communications (RIC) unit 210, and 2) it receives reply packets from the RIC unit 210 and passes the reply back to the computer 212. When the interrogator 202 receives a command from the computer 212, the interrogator 202 either executes the command internally, or transmits the command to the RIC unit 210. The RIC unit 210 then executes the command, but may or may not reply, depending on the command's specific function. When the RIC unit 210 replies, the interrogator 202 passes the reply back to the computer 212. This communication protocol between the RIC unit 210, the interrogator 202 and the computer 212 is well-known in the art.

In one embodiment, the computer 212 is directly connected to the reader 202 by the communications link 216, which may be any type of electrical cable having a parallel or serial port connector for interfacing with the external ports of the computer 212, such as an enhanced parallel port (EPP), RS-232, RS-422 or RS-485 communications line, for example. As mentioned above, the communications link 216 may be any type of well-known communications links, or medium, used for transmitting data from one device to another. In one embodiment, The computer 212 may be located near the reader 202 such that security personnel can view a display screen (not shown) of the computer 212 as people pass through the corridor 204 to verify that each person passing through is not carrying an item which has been reported to be lost or stolen. If a person passing through the corridor 204 is carrying a lost or stolen item, the computer 212 should identify the item and, thereafter notify security personnel by displaying a message on its display screen or providing a visual and/or auditory alarm signal.

Alternatively, the computer 212 may be a local computer 212, that is not located near any one reader 202 but, instead, has many readers 202 coupled to it, each reader monitoring a different checkpoint. In this scenario, each reader 202 at each checkpoint requires a means for alerting security personnel stationed at each of the checkpoints. This function can be performed in a number of different ways. For example, an operator monitoring the local computer 212 can call, via telephone, intercom, radio, etc., security personnel located at a particular checkpoint with instructions. Alternatively, the local computer 212 may send an alarm signal to a device located near the particular checkpoint which can provide a visual and/or auditory alarm signal to security personnel stationed at the checkpoint.

As shown in Figure 2, the anti-theft/retrieval system 200 may further include a central database 218 which is coupled to the local computer 212 by a communications link 220. The communications link 220 may be any one of various well-known communications links or mediums which can be used to transmit data from one device to another. As described in further detail below, a primary function of the central database 218 is to store a master list of lost or stolen devices and periodically update a

local list of lost or stolen devices contained within the database 214 of the local computer 212.

Referring to Figure 3, the central database 218 (Fig. 2) may be a computer server 218 which is connected via a computer network 300, to many local computers 212. Each local computer 212 may in turn be interfaced with one or more readers 202, each reader 202 being responsible for monitoring a specified area, or checkpoint, as described above. Any well-known communications protocol, such as the Ethernet communications protocol, may be used to transmit data between each of the multiple local computers 212 and the central server 218. The computer network 300 may be a local area network (LAN), a wide area network (WAN), or alternatively, a part of the global computer information network, otherwise known as the internet.

In order to police for lost or stolen items, a system must be established to report and record lost and stolen items in an efficient and timely manner. For example, after an owner of an item has reported the item to be stolen, its serial number, or other identifying information, should be promptly stored in the central database 218 and provided to each of the local computers 212 to enable them to monitor for the item within a relatively short time after it has been reported to be lost or stolen. Therefore, in one embodiment, the database 214 within the computer 212 is periodically updated with the latest list of lost or stolen goods from the central database 218. The frequency of these updates can be responsive to addition or deletion of an item from the master list stored in the central database 218, or alternatively, the update can occur at predetermined time intervals.

For example, when an owner of a laptop computer discovers that his or her laptop is lost or stolen, the owner can report the missing item to a manufacturer, dealer, or other authorized agent, who can then add the lost/stolen computer to the list of lost/stolen items in the central database 218. The authorized agent may then input the lost/stolen computer's serial number into the central database 218. This serial number is the information, or at least part of the information, which is transmitted by the transmitter 210 (Fig. 2) which is contained in the laptop computer. Additional information transmitted by the transmitter 210 may be the name and address of the registered owner of the laptop computer, for example.

When a person carrying the lost/stolen laptop computer attempts to pass through a checkpoint, represented by corridor 204 in Figure 2, the reader 202 receives the serial number transmitted by the transmitter 210 and forwards this serial number to the computer 212 for comparison with the list of lost or stolen items. If there is a match, the computer 212 generates an alarm signal which is communicated to proper authorities.

After a lost or stolen laptop computer has been retrieved, its serial number, or other identifying information should be removed from the master list of lost or stolen devices. When local lists are updated by the master list, the retrieved laptop computer will also be removed from all local lists of lost or stolen devices.

For security reasons, the list of lost or stolen goods should only be accessible by authorized personnel. In one embodiment, to add or delete an item from the list of lost or stolen items which is stored in the central database 218, a person must provide a password to verify and authenticate his or her identity. Only after such a password is received and verified can that person obtain access to the central database 218. It is also contemplated that the owner of the laptop computer will be able to personally call a "hotline" telephone number that allows the owner to add the serial number of his or her lost laptop computer to the master list of lost or stolen goods, after passing certain security measures, such as entering a registered password, for example.

Referring to Figure 4, a perspective view of a portable computer 400 is illustrated. The computer 400 includes a transmitter 210 located within the housing of the computer 400. As mentioned above, the transmitter 210 may be an RFID tag, which is well-known in the art, or a MicroStamp RIC unit, manufactured by Micron Communications, Inc. However, other types of transmitters which are compact in size and capable of transmitting information at desired frequencies and ranges may be utilized in accordance with the invention.

The transmitter 210 should be permanently attached to an internal portion of the computer 400 so as to not be easily accessible. Therefore, a thief would not be able to circumvent the security features provided by the transmitter 210 by simply removing the transmitter 210. In one embodiment, the transmitter 210 is embedded in the housing of the computer 400 during its manufacture. Since typical radio frequency devices are

capable of transmitting and receiving data when encapsulated by plastic, or other similar materials, encapsulating the transmitter 210 within a portion of the housing of the computer 400, will not significantly degrade the performance of the transmitter 210.

After the transmitter 210 is programmed with a serial number, or other identifying information, related to the computer 400, the transmitter 210 can transmit this information. In one embodiment, this information may be programmed into the memory of the transmitter 210 by utilizing a designated reader 202 (Figs. 2 and 3) to transmit the information to the transmitter 210 and store the information in a memory of the transmitter 210. In one embodiment, for security purposes, the designated reader 202 may be required to provide a password which allows it to write to the memory of the transmitter 210, or alternatively, the information transmitted by the reader 202 may be encrypted such that only the transmitter 210 can read and store the information. Such methods of programming RFID/RIC transmitters are well-known in the art. However, any well-known method of programming the transmitter 210 may be utilized in accordance with the invention.

Once the identifying information has been stored in the memory of the transmitter 210, it should be unalterable, except by authorized personnel and/or the registered owner of the item containing the transmitter 210. Any well-known method of ensuring the integrity of the information stored in the transmitter 210, such as password protection and/or encryption schemes, may be utilized in accordance with the invention.

As described above, the invention provides a method and system which utilizes radio frequency technology to identify lost or stolen goods that randomly come within range of a reader capable of receiving information transmitted by a radio frequency transmitter permanently fixed within the lost or stolen goods. After identifying an item which has been reported to be lost or stolen, the method and system notifies designated personnel, as necessary.

The invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims, rather than by the foregoing description. All changes

which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

5